Understanding how the latest changes to California privacy law may impact New York companies

By: Anna Mercado Clark and Maria Althea Teves
Phillips Lytle LLP

Businesses located in and outside of California may be subject to additional obligations pursuant to the California Consumer Privacy Act (CCPA), as amended this year. The amendments include steeper fines for violations of the CCPA and its accompanying regulations. The CCPA amendments also modify existing rights, while additional proposed regulatory changes impose new obligations regarding cybersecurity audit record retention, risk assessment deadlines, and procedures for utilizing automated decision-making technology (ADMT), among other things. This article highlights some amendments of interest that took effect on Jan. 1, 2025, as well as regulatory proposals that may take effect as early as Oct. 31, 2025.


Anna Mercado Clark
Partner


Maria Althea Teves
Attorney

Covered businesses that meet certain threshold revenue and activity requirements, share common branding with a business subject to the CCPA, or have certain business relationships with other companies subject to the CCPA, should pay attention to these amendments, with more on the horizon.

Increased fines

Fines for certain violations increased as follows:

- **Unintentional violation**: Fine increased from $2,500 to $2,663 per violation.
- **Intentional violation**: Fine increased from $7,500 to $7,988 per violation.
- **Intentional violations involving minors:** Fine of $7,988 per violation for those involving minors under 16 years of age.
- **Civil penalties**: Civil penalties for each person per incident range from $107 to $799, whichever is greater.

New obligations of covered businesses

The amendments also modify existing rights of and add obligations imposed on businesses. Those obligations include:

- **Neural data**: This information, generated by measuring activity of the nervous system, is considered "sensitive personal information." The same privacy protections afforded to sensitive personal information (e.g., precise geolocation, citizenship, racial or ethnic origin) extend to neural data, including consent to collect or use and complying with requests to delete or opt out of sharing.
- **Opt-out in mergers**: Entities that acquire other businesses through mergers and acquisitions must honor opt-out requests made to the acquired company.

The California Privacy Protection Agency (CPPA), a state agency established to implement and enforce the CCPA, also proposed regulatory changes that would create new obligations on businesses which may take effect later this year:

- **Audit record retention**: A covered business, not just the auditor, must now keep a record of its annual cybersecurity audits for at least five years.
- **Risk assessment**: While no deadline previously existed, covered businesses must now update their privacy risk assessments within 45 days of any material change (that introduces new risks or may weaken personal data protections) in data processing activities.
- **ADMT**: Covered businesses will be required to provide information about their use of ADMT in significant decision-making (e.g., financial services, employment screening, pricing) upon a resident's request. Businesses must also accommodate a resident's appeal of the business's use of ADMT or opt out of ADMT.

The proposed regulatory amendments are subject to change based on comments submitted to the CPPA after the time of writing.

Compliance strategy

Businesses need to determine whether they are subject to the CCPA directly or through entities with which they have business relationships. To assist in this analysis and in developing a compliance program, businesses should consider their data collection, processing and transfer activities, evaluate sufficiency of risk assessment and audit procedures, and review opt-out mechanisms. To assist in this process, experts who are well-versed in these issues and your industry may be particularly helpful.

Anna Mercado Clark, Partner and Chief Information Security Officer at Phillips Lytle, is the Co-Leader of the firm's Technology Industry Team. She can be reached at aclark@phillipslytle.com or 212-508-0466.

Maria Althea Teves, attorney at Phillips Lytle, focuses her practice on cybersecurity and commercial litigation. She can be reached at mteves@phillipslytle.com or 716-847-5415.